UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/499,633	02/08/2000	Young-Soon Cho	0630-0981P	1525

7590 01/13/2004

Birch Stewart kolasch & Birch LLP
P O Box 747
Falls Church, VA 22040-0747

EXAMINER	
LE, DAVID Q	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 01/13/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/499,633	CHO ET AL.
	Examiner	Art Unit
	David Q Le	3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 September 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4 and 19-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4 and 19-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Examiner's Note

1. The Examiner has pointed out particular references contained in the prior art of record in the body of this action for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other passages and figures apply as well. It is requested from the Applicant, in preparing the response, to consider fully the entire references as well as the context of all reference passages as potentially teaching all or part of the claimed inventions.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 15 October 2003 has been entered. An action on the RCE follows.

Status of Claims

3. As requested in the RCE filed on 30 September 2003, the Amendment After Final Rejection and Request for Consideration previously filed on 28 July 2003 under 37 CFR § 1.111 was considered and has been entered:

Claims 1 and 2 were amended.
Claims 5-18 were deleted.
Claims 19-36 were added.

Claims 1-4 and **19-36** are now pending.

Response to Request for Reconsideration

4. The amendment filed on 28 July 2003 under 37 CFR § 1.111 has been considered but is ineffective to overcome ***Schneck et al***., US Patent No 5,933,498.

Response to Arguments

5. Applicant's arguments have been fully considered but they are not persuasive.

As per **claim 1**.
Applicant argues that Schneck does not teach that
a) an encryption key is generated in a digital data player; this key being based on
b) an identification number of the data storage medium, or
c) an identification number of the digital data playing device.

Examiner disagrees with this reading of Schneck.
First off, Schneck's invention is directed to a system, method, and apparatus for controlling access and distribution of digital property (Abstract; Summary of the Invention). The main devices in this system comprise a secure authoring/access mechanism which can encrypt protected digital data, as well as the encryption key used in that encryption and the rules governing the access of and use of that data (Fig 1-5, 14-15; associated text; Col 15, L19-38; Col 16, line 64 – Col 17, line 5; Figs 8-12). This authoring/access mechanism may reside within a distributor, authoring, or publishing computer system, and it may also exist inside a user computer system, so that the user may read/play protected digital data provided by the distributor, author, or publisher (Fig 8, [block] "168 Encryption Hardware"; associated text, Col 15, lines 30-63). When the apparatus serves as a user device, it is thus a digital data player (a).

Next, turning to the encryption of the digital data to be distributed, Schneck teaches that the encryption algorithm selected by the distributor, author, or publisher may vary in complexity and degree of

security, depending on the value put upon the data to be protected (Col. 12, lines 27-48). Corresponding to this value and risk assessment, the distributor, author, or publisher may also pick various methods for generating the encryption key(s) used to actually encrypt the data (D), the data encrypting key itself (K_D), the rules (R) governing the access to and use of the data, thus ending up with either a K_D or a K_D *and* a K_R (Fig 4, associated text; Col 12, lines 1-16). Again, depending on the application, Schneck discloses that these keys may be generated – first by the distributor, author, or publisher, then recreated by an similar algorithm within the user's access system – so that the data, the data key, and the data rules can be securely encrypted, and subsequently decrypted at the user's computer system (Col. 12-18: "The Authoring Mechanism"; "The Access Mechanism").

Schneck goes on to teach that these keys may be derived from:

(i) the packaged digital product (Col. !2, lines 4-6: "[key] ..is different for each product (i.e. for each packaged data.." - i.e. the digital data medium being distributed; or

(ii) the key(s) may be common to a whole class of systems (Col 12, lines 10-12: "..is the same for all products and all embodiment of the systems.."; or, yet another possibility,

(iii) the keys may be "..unique for each version of the system [sold]" (Col. 12, lines 12-16);

(iv) for very valuable, high security products, Schneck teaches that the key(s) may be generated "[uniquely] for each item of data to be distributed" (Col. 12, lines 43-48).

One can readily see from the above that, depending on which encryption option is picked, the encrypting key(s) may be computed from algorithms utilizing either product identification numbers (software), serial numbers (of individual media or machines), certified digital signatures (from systems machines, users), or any other ID uniquely associated with the data, distribution medium, player device, or end-user (above citations; Col 14, lines 35-50), or combination thereof. Schneck even talks briefly about the ID of a publisher, albeit not directly used as a seed to generate an encryption key (Col 13, lines 27). As such, it is clear that the reference has taught the remaining two limitations (b) and (c) that Applicant claims are distinguishing features of his invention.

As per **claims 2-14**.

Here again, Examiner disagrees with Applicant. The Schneck citations used for the 35 USC § 102(e) rejection of claim 1 and the 35 USC § 103(a) rejections of claims 2-14 clearly show that Schneck was very deliberate in teaching that:

(1) the preferred embodiment of his invention would use encryption based on either numbers uniquely identifying the data to be protected itself, the unique IDs of the various parts of a user's device, or a combination thereof, with further participation of a trusted third party certification agency, if the application warrants all such measures, and

(2) the encryption functions may be performed in any chosen device, whether at a content creator's site, distributor's site, or at an authorized user's site, without sacrificing any of the security measures central to his system and method; see Schneck: C28, L20-24: "..a standard computer" [i.e. a digital data playing device] "equipped with an access mechanism 114 will function as an authoring/distribution system".

The motivation for setting up a system wherein a digital data playing device performs such encryption functions, as taught by Schneck, is therefore obvious: a very desirable, secure, hard to breach protection and control system for proprietary digital content, with no significant sacrifice in flexibility and ease of use.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) do not apply to the examination of this application as the application being examined was not (1) filed on or after November 29, 2000, or (2) voluntarily published under 35 U.S.C. 122(b). Therefore, this application is examined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

7. **Claims 1, 24, and 33** are rejected under 35 U.S.C. 102(e) as being anticipated by **Schneck et al**, US Patent No 5,933,498, issued Aug 3, 1999 and filed on Nov 5, 1997.

Schneck describes an method, system and apparatus for controlling access to/encrypting/decrypting/playing digital data (Fig 1; Col 7, lines 8-55) with features and functionalities that meet all the limitations of claims 1, 24, and 33:

An apparatus ...encrypted digital data file (Schneck's "access mechanism"; see citations in previous section), *comprising:*

a digital data playing device for receiving the encrypted digital data file, storing the encrypted digital data file in a data storage medium, and decrypting the stored digital data file using an encryption key (Fig 8; Col 15, lines 19-38; Figs 9-12), *wherein*

the encryption key is generated in the digital data playing device on the basis of
[claim1] an identification number of the data storage medium or an identification number of the digital data playing device (Col 14, lines 32-50).
[claim 24] an ID number of the digital data playing device.
[claim 33] a combination of ...ID numbers of the data storage medium and the digital data playing device (see citations in above section).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. **Claims 2-4, 19-23, and 34-36** are rejected under 35 U.S.C. 103(a) as being unpatentable over ***Schneck***.

As per **claims 2, 19, 25, 28, and 34**:

Schneck discloses that data distributed via his system may be protected by encrypting the data with a "data-encrypting key K_D". This K_D may be the same for all copies of the packaged data. This K_D may be further encrypted by a "rules-encrypting key K_R", wherein K_R is unique to each version of the system or each receiving player/computer of each user (Fig 4; Col 12, lines 1-16). Schneck further discloses that the algorithms used in the generation and application of said encrypting keys might be selected from many established encryption algorithms, depending on the assessment of risks and degree of protection of the data desired (Col 12, lines 27-48). Additionally, Schneck discloses that the serial number of a device may be used in the generation of his rules-encrypting key K_R (Col 14, lines 31-50).

Schneck does not specifically recite all the various identification numbers that may be used in generating the encryption key used to encrypt the data.

However, Schneck teaches that effective protection of the data may be accomplished by encrypting the data and rules governing its access using one or more encryption keys, each generated by using unique IDs associated with the product distributed, its storage medium, player device, end user, product publisher, and/or any combination of these numbers.

Therefore it would have been obvious for one ordinarily skilled in the art at the time the invention was made to have applied Schneck's teachings (see all above citations) to create an apparatus wherein

the encryption key includes information regarding
[claim 2] a manufacturing company of the data storage medium
[claim 19] a serial number of the data storage medium
[claim 25] a manufacturing company of the digital data playing device
[claim 28] a serial number of the digital data playing device
[claim 34] a combination of a manufacturing company and a serial number of the data storage medium and the digital data playing device.

Such an embodiment would meet the limitations of claim 2, and would have been motivated by a desire to very specifically control access to data being distributed, according to each specific user or class of user (each user having bought a player device from a specific manufacturer, each such player uniquely identified by its serial number).

As per **claims 3, 26, and 29**:

As the references cited above show, Schneck discloses that encryption keys used in his system may be derived using many different, well known encryption algorithms. Using additional arbitrary values in such encryption algorithms (i.e. semi-random or random numbers) is well known within the art. Therefore it would have been obvious to one ordinarily skilled in the art at the time the invention was made that a system could have been set up with

the encryption key further including an arbitrarily set value,

for the purpose of making the transmitted encrypted data harder to crack thus better protected.

As per **claims 4, 21, 27 and 30**:

Schneck discloses that the playing device in his system may be configured so that all data is protected by encryption within an "access mechanism" (Figs 8, 9, 10b, 11; Col 15, line 19 – Col 17, line 33).

Therefore it would have been obvious to one ordinarily skilled in the art at the time the invention was made to have set up an apparatus

further comprising: a processor for decrypting a previously encrypted digital data file and reproducing the digital data file, or re-encrypting the decrypted digital data file using the encryption key and transmitting the re-encrypted digital data file to the digital data playing device.

This would have been done to further protect the data from being misused or illegally intercepted, copied, or transmitted at the user's end. Even when being transmitted from a processor that received the data to a playing device, the data would be encrypted and thus protected.

As per **claims 22, 31 and 35**.
Schneck does not specifically recite
the digital data playing device is an MP3 player.

However he does disclose that any type of digital data may be used in his system (Col 11, lines 50-58). Therefore it would have been obvious that MP3, a compressed digital audio file format, would inherently be included in the data that could be protected and used in a system based on Schneck's invention.

As per **claims 23, 32, and 36**.
Schneck doesn't specifically recite
the data storage medium is a removable medium.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Q Le whose telephone number is 703-305-4567. The examiner can normally be reached on 8:30am-5:30pm Mo-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James P Trammell can be reached on 703-305-9768. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-1113.

DQL